

SIEVA



Evaluando la visibilidad de tu SIEM

JT RedIris - Zaragoza
15/06/2023

Nil Ortiz - Senior R&D Cybersecurity Engineer



Never stop
designing the
digital future

i2CAT.net   



Whoami



Nil Ortiz

Senior R&D Cybersecurity engineer

Incident response and threat intelligence analysis

Msc. in Cybersecurity

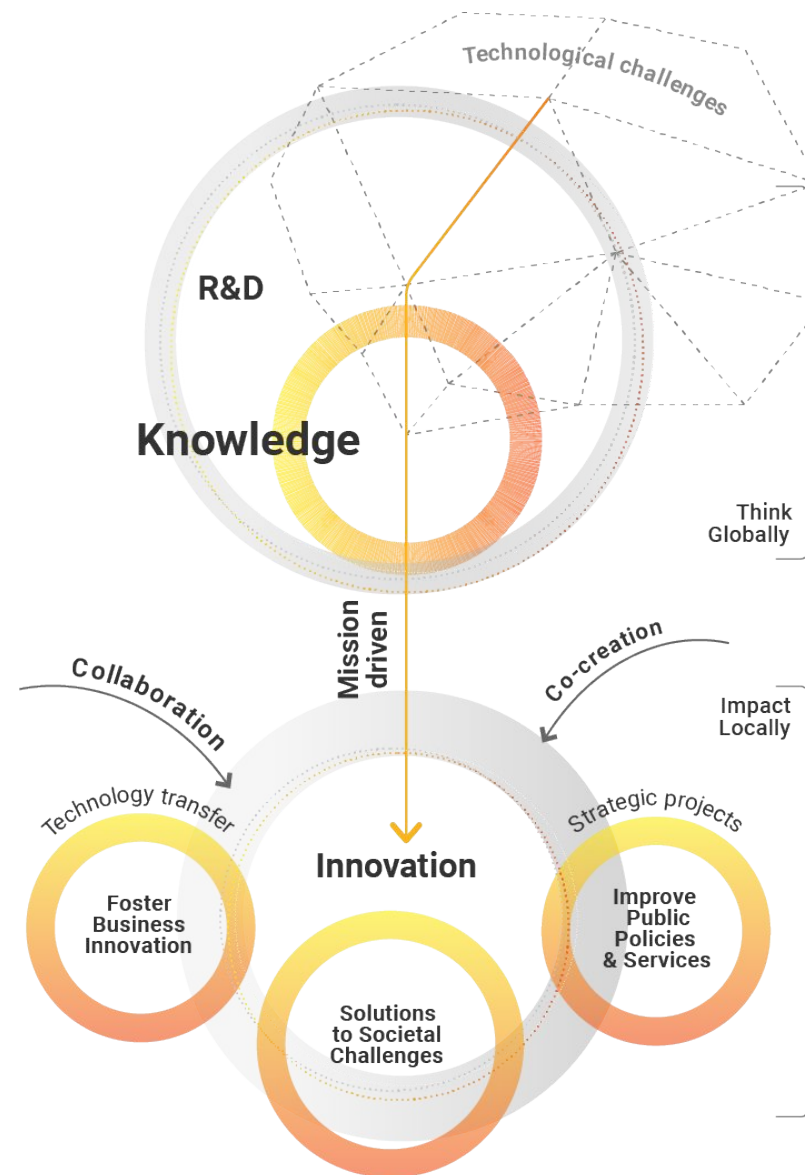
nil.ortiz@i2cat.net [LinkedIn/in/nilortiz/](https://www.linkedin.com/in/nilortiz/)



i2CAT



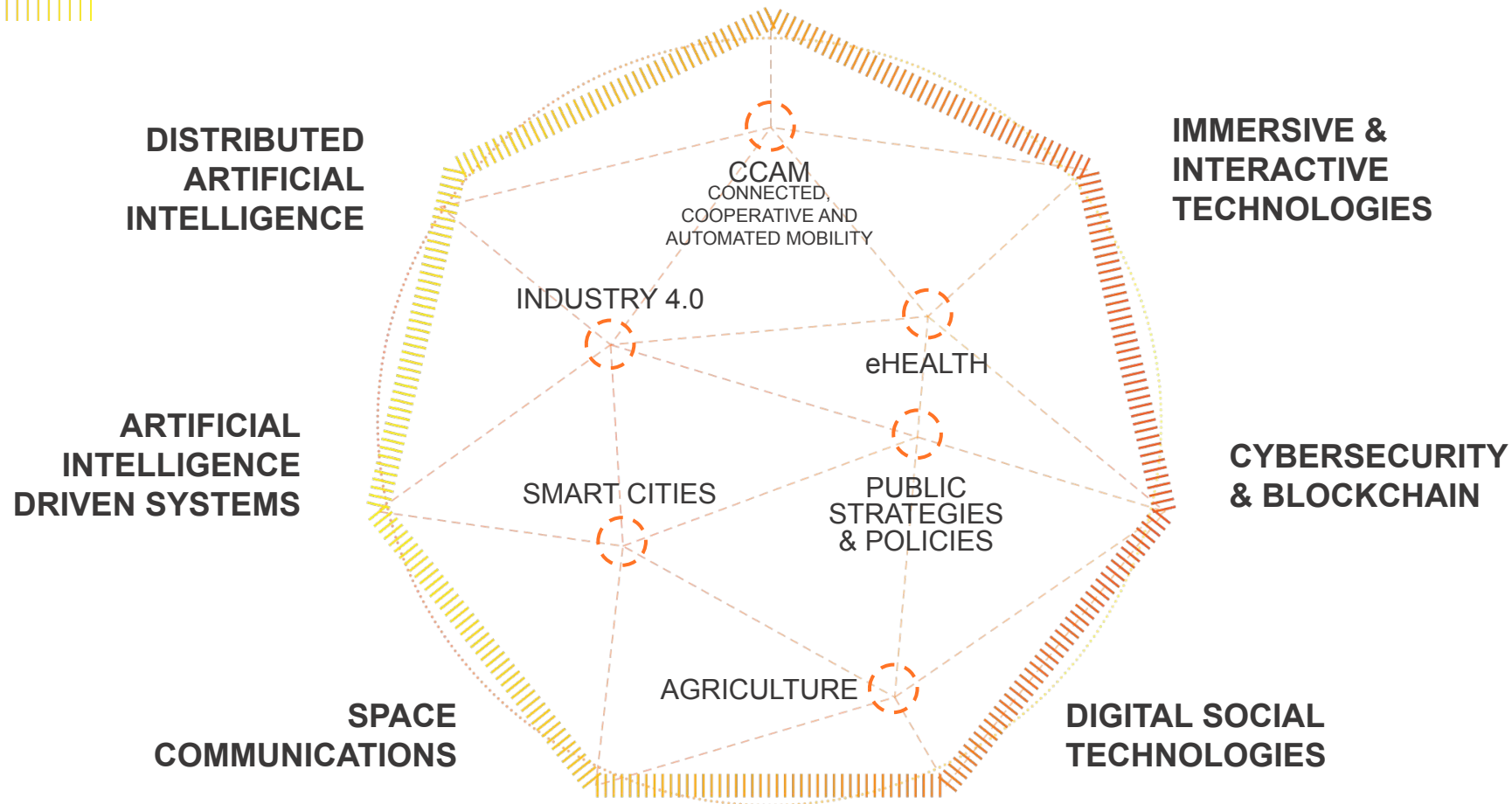
i2CAT es un centro de investigación centrado en proyectos impulsados por una misión para abordar el desafío de diseñar la sociedad digital del futuro basada en la investigación y la innovación en tecnologías digitales avanzadas.



Áreas de Investigación e Innovación



SMART NETWORKS AND SERVICES
6G, 5G, IoT



Iniciativas cyber + IA



DetectUEBA (Threat-Centric ML for Detection capabilities)

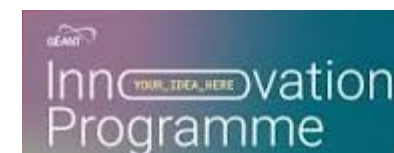
- Adopción de proxies de explicabilidad para la detección de amenazas
- Alinear la salida de un modelo ML con MITRE ATT&CK

openUEBA (User-Centric ML for prevention capabilities)

- Determinar patrones de comportamiento en datos históricos de usuarios
- Calcular el riesgo de una amenaza dentro de una infraestructura

SIEVA

- Evaluación de visibilidad para SIEMs
- Veamos esta herramienta en detalle ...



Limited disclosure, restricted to participants' organizations.



i2cat^R

THE INTERNET
RESEARCH CENTER

SIEVA



Contexto



- La mayoría de las organizaciones utilizan SIEMs como la piedra angular de sus operaciones de seguridad
- Los SIEM administran todos los datos relacionados con la seguridad y generan alertas basadas en reglas
- Para desarrollar reglas, es necesario comprender qué información se requiere de cada fuente de datos disponible

Problema



- Los SIEM son herramientas muy complejas que deben configurarse y mantenerse adecuadamente
- Los ingenieros de seguridad dedican mucho tiempo a tareas relacionadas con la ingeniería de datos.
- Las organizaciones tienen dificultades para comprender sus propias necesidades y capacidades de monitoreo

Solución



- SIEVA es una herramienta para evaluar la visibilidad de un SIEM sobre una red contra el marco MITRE ATT&CK.
- No realiza detección, análisis, prevención, gestión de riesgos ni nada más que evaluar la visibilidad.
- Reduce la carga de trabajo de los ingenieros de seguridad que se encargan de las tareas de ingeniería de datos.
- Permite a C-suite definir mejor las estrategias a largo plazo con respecto a sus necesidades de monitoreo.

MITRE ATT&CK Framework



MITRE **ATTACK** Framework es una base de conocimiento que rastrea las **tácticas** y **técnicas** de los adversarios utilizadas por los actores maliciosos a lo largo de todo el ciclo de vida del ataque.

Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 9 techniques	Execution 13 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 42 techniques	Credential Access 17 techniques	Discovery 30 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Active Scanning (3)	Acquire Infrastructure (7)	Drive-by Compromise	Command and Scripting Interpreter (8)	Account Manipulation (5)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Adversary-in-the-Middle (3)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (3)	Application Layer Protocol (4)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Compromise Accounts (3)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (3)	Compromise Infrastructure (7)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (14)	Boot or Logon Autostart Execution (14)	BITS Jobs	Credentials from Password Stores (5)	Browser Bookmark Discovery	Lateral Tool Transfer	Audio Capture	Data Encoding (2)	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Gather Victim Network Information (6)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (5)	Boot or Logon Initialization Scripts (5)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Automated Collection	Data Obfuscation (3)	Exfiltration Over C2 Channel	Data Manipulation (3)
Gather Victim Org Information (4)	Establish Accounts (3)	Phishing (3)	Inter-Process Communication (3)	Browser Extensions	Boot or Logon Initialization Scripts (5)	Debugger Evasion	Forced Authentication	Cloud Service Dashboard	Remote Services (6)	Browser Session Hijacking	Dynamic Resolution (3)	Exfiltration Over Other Network Medium (1)	Defacement (2)
Phishing for Information (3)	Obtain Capabilities (6)	Replication Through Removable Media	Native API	Compromise Client Software Binary	Create or Modify System Process (4)	Deobfuscate/Decode Files or Information	Forge Web Credentials (2)	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Encrypted Channel (2)	Exfiltration Over Physical Medium (1)	Disk Wipe (2)
Search Closed Sources (2)	Stage Capabilities (6)	Supply Chain Compromise (3)	Scheduled Task/Job (5)	Create Account (3)	Domain Policy Modification (2)	Deploy Container	Input Capture (4)	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage	Fallback Channels	Exfiltration Over Web Service (2)	Endpoint Denial of Service (4)
Search Open Technical Databases (3)	Trusted Relationship	Serverless Execution	Serverless Execution	Create or Modify System Process (4)	Escape to Host	Direct Volume Access	Modify Authentication Process (7)	Container and Resource Discovery	Taint Shared Content	Data from Configuration Repository (2)	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
Search Open Websites/Domains (3)	Valid Accounts (4)	Shared Modules	Shared Modules	Event Triggered Execution (16)	Event Triggered Execution (16)	Domain Policy Modification (2)	Multi-Factor Authentication Interception	Debugger Evasion	Use Alternate Authentication Material (4)	Data from Information Repositories (3)	Multi-Stage Channels	Transfer Data to Cloud Account	Inhibit System Recovery
Search Victim-Owned Websites		Software Deployment Tools	Software Deployment Tools	Exploitation for Privilege Escalation	Exploitation for Privilege Escalation	Execution Guardrails (1)	Multi-Factor Authentication Request Generation	Domain Trust Discovery		Data from Local System	Non-Application Layer Protocol	System Shutdown/Reboot	Network Denial of Service (2)
		System Services (2)	System Services (2)	Hijack Execution Flow (12)	Hijack Execution Flow (12)	Exploitation for Defense Evasion		File and Directory Discovery		Data from Network Shared Drive	Non-Standard Port	Resource Hijacking	Service Stop
		User Execution (3)	User Execution (3)	Hide Artifacts (10)	Hide Artifacts (10)	File and Directory Permissions Modification (2)		Group Policy Discovery		Proxy (4)	Protocol Tunneling		
		Windows Management	Windows Management	Hijack Execution Flow (12)	Hijack Execution Flow (12)	Hide Artifacts (10)		Network Service Discovery					
				Process	Process	Hijack Execution Flow (12)		Network Share Discovery					



Arquitectura



Arquitectura



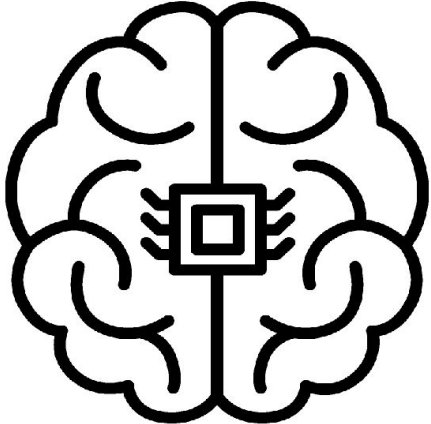
```

> message: 1157689387.862 2 10.105.21.199 TCP_HIT/200 7256 GET http://us.11.yimg.com/us.yimg.com/1/us/pim/dclient/d/img/md5/3c2490743689664662d0a03988cdf96_1.gif badeyek NONE/- image/gif
_id: Y3rci4IBFuzzTzY2qyHi _index: webproxy-squid _score: 1 _type: _doc

> message: 112.66.83.11 - - [12/Jan/2017:17:06:01 -0800] "GET /Security-Data-Analysis/Lab_1/conn_log.zip HTTP/1.1" 206 721266 "-" "Mozilla/5.0 (Linux; Android) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/34.0.1847.131 Safari/537.36" _id: t23kPoIBFuzzTzY2R7-M _index: webservice-generic _score: 1 _type: _doc

> message: Jan 20 05:59:00 198.24.1.30 dhdpd[8738]: Forward map update for 172.25.172.0 abandoned because of non-retryable failure: NXRRSET _id: V3exWIIIBFuzzTzY2nJiI _index: dhcp-server-linux _score: 1
_type: _doc

> message: date=2022-08-29 time=09:42:45 eventtime=1661758965179985415 tz="+0200" logid="000000013" type="traffic" subtype="forward" level="notice" vd="root" srcip=172.26.211.181 srcport=50595
srcintf="ssl.root" srcintfrole="undefined" dstip=172.26.211.181dstport=443 dstintf="PublicVLAN" dstintfrole="wan" srccountry="Reserved" dstcountry="United States" sessionId=33905922 proto=6 action="close"
policyid=7 policitype="policy" poluid="57d3e5c2-9c66-51eb-0af1-2582f407571e" policyname="vpn_VPNSSLPortalToInternet" user="nil_ortiz" groups="ipsec_users" service="HTTPS" transisp="snat" transip=172.26.211.181
transport=50595 duration=1 sentbyte=3235 rcvbyte=1831 sentpkt=9 rcvdpkt=9 appcat="uncanned" _id: Sobj6IIBFuzzTzY2XZiJ _index: firewall-fortigate _score: 1 _type: _doc
    
```



TA0043 Reconnaissance 10 techniques	TA0042 Resource Development 7 techniques	TA0001 Initial Access 9 techniques	TA0002 Execution 12 techniques	TA0003 Persistence 19 techniques	TA0004 Privilege Escalation 13 techniques	TA0005 Defense Evasion 39 techniques	TA0006 Credential Access 15 techniques	TA0007 Discovery 27 techniques	TA0008 Lateral Movement 9 techniques	TA0009 Collection 17 techniques	TA0011 Command and Control 16 techniques	TA0010 Exfiltration 9 techniques	TA0040 Impact 13 techniques
T1595 Active Scanning	T1583 Acquire Infrastructure	T1189 Drive-by Compromise	T1059 Command and Scripting Interpreter	T1098 Account Manipulation	T1548 Abuse Elevation Control Mechanism	T1548 Abuse Elevation Control Mechanism	T1110 Brute Force	T1087 Account Discovery	T1210 Exploitation of Remote Services	T1560 Archive Collected Data	T1071 Application Layer Protocol	T1020 Automated Exfiltration	T1531 Account Access Removal
T1592 Gather Victim Host Information	T1586 Compromise Accounts	T1190 Exploit Public-Facing Application	T1609 Container Administration Command	T1197 BITS Jobs	T1134 Access Token Manipulation	T1134 Access Token Manipulation	T1555 Credentials from Password Stores	T1010 Application Window Discovery	T1534 Internal Spearphishing	T1123 Audio Capture	T1092 Communication Through Removable Media	T1030 Data Transfer Size Limits	T1485 Data Destruction
T1589 Gather Victim Identity Information	T1584 Compromise Infrastructure	T1133 External Remote Services	T1610 Deploy Container	T1547 Boot or Logon Autostart Execution	T1197 BITS Jobs	T1197 BITS Jobs	T1212 Exploitation for Credential Access	T1217 Browser Bookmark Discovery	T1570 Lateral Tool Transfer	T1119 Automated Collection	T1132 Data Encoding	T1048 Exfiltration Over Alternative Protocol	T1486 Data Encrypted for Impact
T1590 Gather Victim Network Information	T1587 Develop Capabilities	T1200 Hardware Additions	T1203 Exploitation for Client Execution	T1037 Boot or Logon Initialization Scripts	T1547 Boot or Logon Autostart Execution	T1612 Build image on Host	T1187 Forced Authentication	T1580 Cloud Infrastructure Discovery	T1563 Remote Service Session Hijacking	T1115 Clipboard Data	T1801 Data Obfuscation	T1041 Exfiltration Over C2 Channel	T1565 Data Manipulation
T1591 Gather Victim Org Information	T1585 Establish Accounts	T1566 Phishing	T1203 Exploitation for Client Execution	T1176 Browser Extensions	T1037 Boot or Logon Initialization Scripts	T1140 Deobfuscate/Decode Files or Information	T1187 Forced Authentication	T1538 Cloud Service Dashboard	T1021 Remote Services	T1530 Data from Cloud Storage Object	T1568 Dynamic Resolution	T1491 Defacement	
T1598 Phishing for Information	T1598 Obtain Capabilities	T1091 Replication Through Removable Media	T1559 Inter-Process Communication	T1154 Compromise Client Software Binary	T1037 Boot or Logon Initialization Scripts	T1610 Deploy Container	T1606 Forge Web Credentials	T1526 Cloud Service Discovery	T1091 Replication Through Removable Media	T1602 Data from Configuration Repository	T1573 Encrypted Channel	T1011 Exfiltration Over Other Network Medium	T1561 Disk Wipe
T1597 Search Closed Sources	T1608 Stage Capabilities	T1053 Scheduled Task/Job	T1106 Native API	T1136 Create Account	T1543 Create or Modify System Process	T1008 Direct Volume Access	T1056 Input Capture	T1513 Container and Resource Discovery	T1008 Replication Through Removable Media	T1213 Data from Information Resources	T1008 Fallback Channels	T1052 Exfiltration Over Physical Medium	T1499 Endpoint Denial of Service
T1596 Search Open Sources	T1195 Search Open Sources	T1128 Search Open Sources	T1053 Scheduled Task/Job	T1543 Create or Modify System Process	T1484 Domain Policy Modification	T1484 Domain Policy Modification	T1556 Modify	T1482 Domain Trust Discovery	T1072 Software Deployment Tools	T1105 Ingress Tool Transfer	T1105 Ingress Tool Transfer	T1567 Firmware Corruption	T1495 Firmware Corruption



Motor IA - Como funciona?



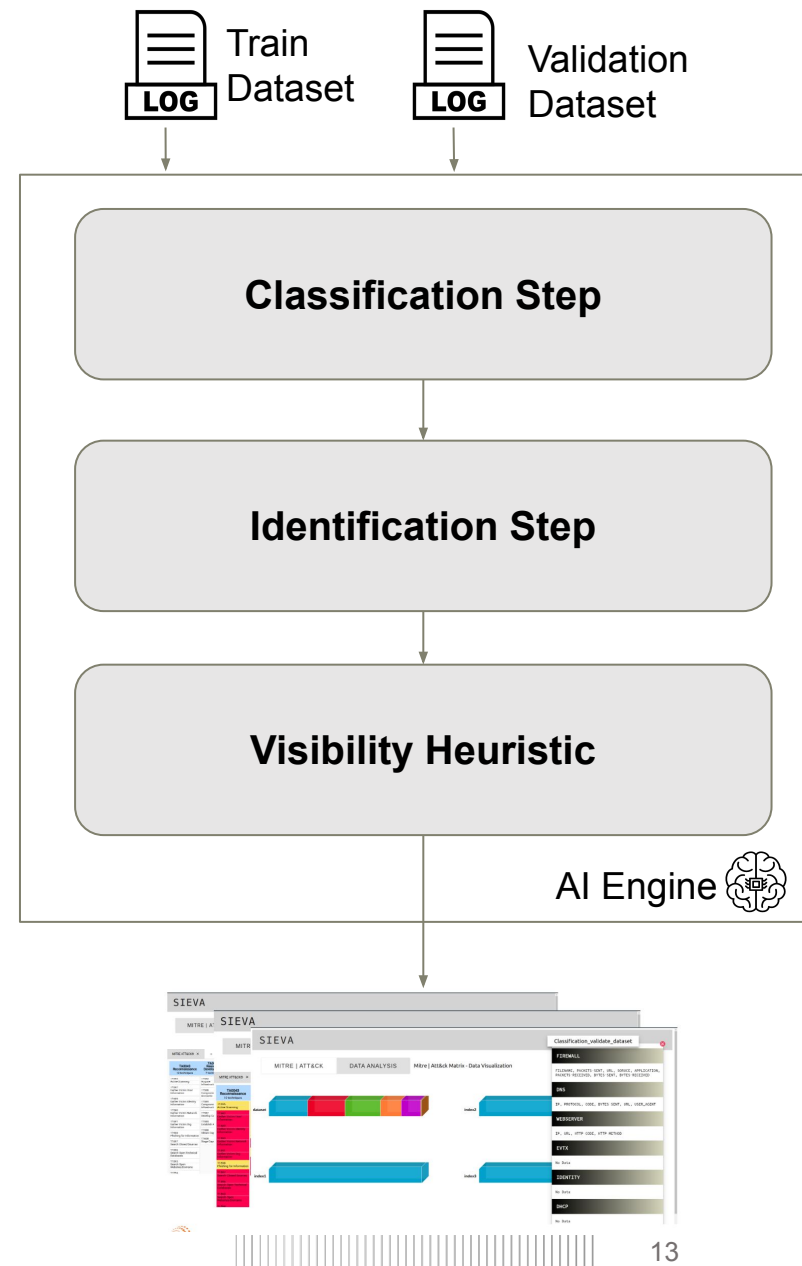
El motor de IA es un procedimiento de tres pasos:

Clasificación: Se utiliza un modelo de clasificación multiclase supervisado para determinar la tipología de registros

Identificación: Se utiliza un modelo NER personalizado para extraer entidades de los registros. *

Heurística: se utiliza la matriz ATT&CK para categorizar los registros según el grado de visibilidad

(*) Un conjunto de datos que contiene registros de diferentes proveedores, se define durante los pasos 1 y 2

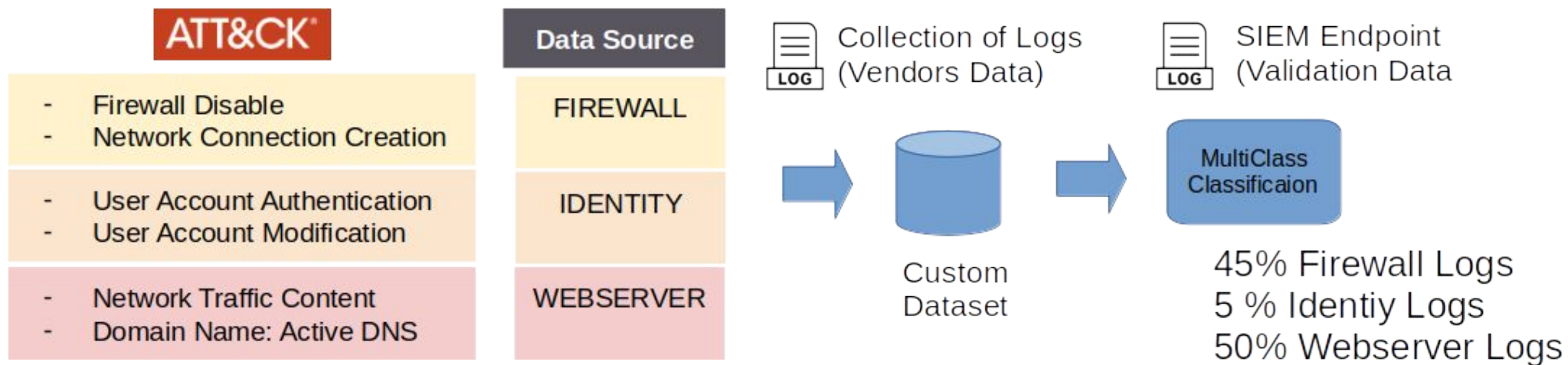


Motor IA - Como funciona?



Clasificación

- Se utiliza un modelo de clasificación para clasificar los registros de acuerdo con las fuentes de datos definidas en MITRE ATT&CK
- Construimos manualmente un conjunto de datos utilizando muestras de registros de diferentes proveedores.

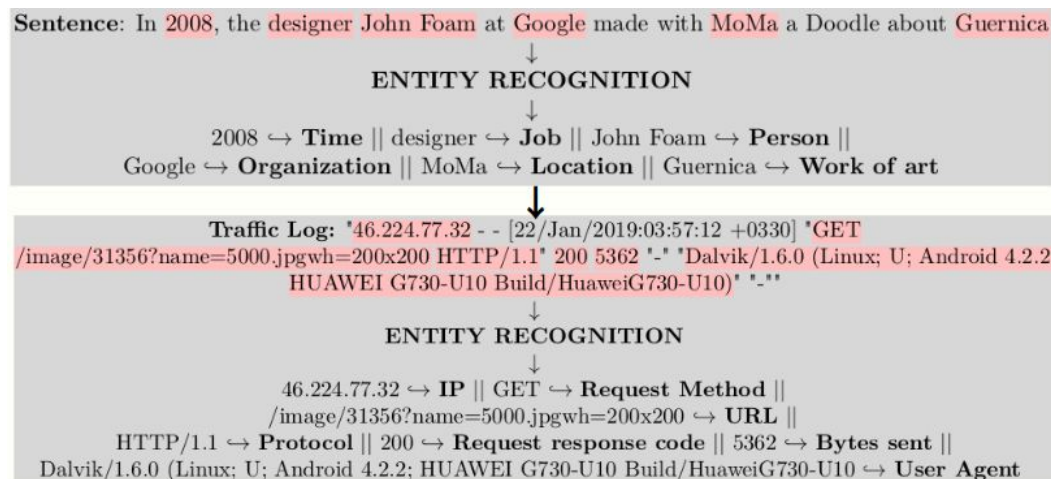


Motor IA - Como funciona?



Identificación

- Las técnicas de reconocimiento de entidades nombradas (NER) buscan localizar y clasificar las diferentes entidades en el texto en categorías predefinidas.
 - Texto plano → Registros sin procesar (RAW)
 - Categorías → IP, Dominios, host..



Modelo NER
común

Modelo NER
personalizado

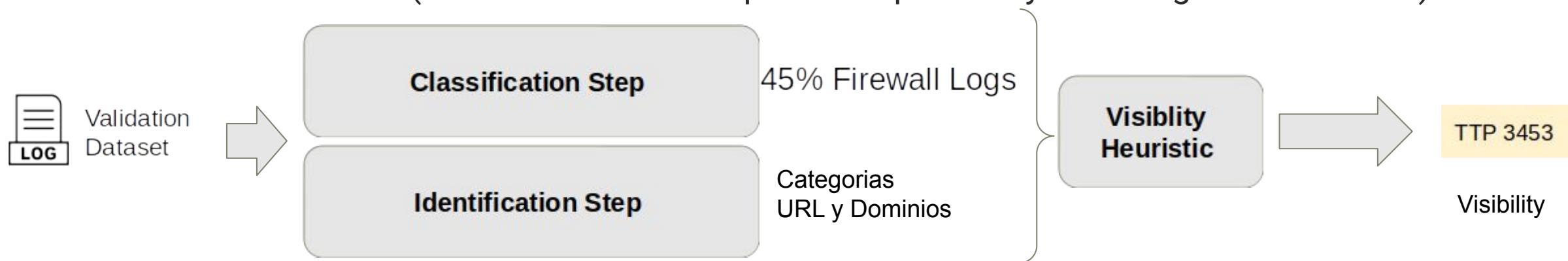


Motor IA - Como funciona?



Heurística

- Poner todo junto usando la representación de la matriz MITRE ATT&CK
- Se establece una heurística para asociar (Fuentes de Datos, Campos) => TTP
 - Visibilidad heurística:
 - (Sin visibilidad → 0% de precisión prevista por clase)
 - (Visibilidad parcial → !0% de precisión prevista por clase)
 - (Visibilidad → !0% de precisión prevista y > n categorías definidas)



Interfaz gráfica



SIEVA

MITRE | ATT&CK

DATA ANALYSIS

Mitre | Att&ck Matrix - Navigator

MITRE ATT&CK® × +

TA0043 Reconnaissance 10 techniques	TA0042 Resource Development 7 techniques	TA0001 Initial Access 9 techniques	TA0002 Execution 12 techniques	TA0003 Persistence 19 techniques	TA0004 Privilege Escalation 13 techniques	TA0005 Defense Evasion 39 techniques	TA0006 Credential Access 15 techniques	TA0007 Discovery 27 techniques	TA0008 Lateral Movement 9 techniques	TA0009 Collection 17 techniques	TA0011 Command and Control 16 techniques	TA0010 Exfiltration 9 techniques	TA0040 Impact 13 techniques
T1595 Active Scanning	T1583 Acquire Infrastructure	T1189 Drive-by Compromise	T1059 Command and Scripting Interpreter	T1098 Account Manipulation	T1548 Abuse Elevation Control Mechanism	T1548 Abuse Elevation Control Mechanism	T1110 Brute Force	T1087 Account Discovery	T1210 Exploitation of Remote Services	T1560 Archive Collected Data	T1071 Application Layer Protocol	T1020 Automated Exfiltration	T1531 Account Access Removal
T1592 Gather Victim Host Information	T1586 Compromise Accounts	T1190 Exploit Public- Facing Application	T1609 Container Administration Command	T1197 BITS Jobs	T1134 Access Token Manipulation	T1134 Access Token Manipulation	T1555 Credentials from Password Stores	T1010 Application Window Discovery	T1534 Internal Spearphishing	T1123 Audio Capture	T1092 Communication Through Removable Media	T1030 Data Transfer Size Limits	T1485 Data Destruction
T1599 Gather Victim Identity Information	T1584 Compromise Infrastructure	T1133 External Remote Services	T1610 Deploy Container	T1547 Boot or Logon Autostart Execution	T1547 Boot or Logon Autostart Execution	T1197 BITS Jobs	T1212 Exploitation for Credential Access	T1217 Browser Bookmark Discovery	T1570 Lateral Tool Transfer	T1119 Automated Collection	T1132 Data Encoding	T1048 Exfiltration Over Alternative Protocol	T1486 Data Encrypted for Impact
T1590 Gather Victim Network Information	T1587 Develop Capabilities	T1200 Hardware Additions	T1203 Exploitation for Client Execution	T1037 Boot or Logon Initialization Scripts	T1037 Boot or Logon Autostart Execution	T1612 Build Image on Host	T1187 Forced Authentication	T1580 Cloud Infrastructure Discovery	T1563 Remote Service Session Hijacking	T1115 Clipboard Data	T1001 Data Obfuscation	T1041 Exfiltration Over C2 Channel	T1565 Data Manipulation
T1591 Gather Victim Org Information	T1585 Establish Accounts	T1566 Phishing	T1559 Inter-Process Communication	T1176 Browser Extensions	T1037 Boot or Logon Initialization Scripts	T1140 Deobfuscate/Decode Files or Information	T1606 Forge Web Credentials	T1538 Cloud Service Dashboard	T1021 Remote Services	T1530 Data from Cloud Storage Object	T1568 Dynamic Resolution	T1491 Defacement	
T1598 Phishing for Information	T1588 Obtain Capabilities	T1091 Replication Through Removable Media	T1106 Native API	T1554 Compromise Client Software Binary	T1543 Create or Modify System Process	T1610 Deploy Container	T1056 Input Capture	T1526 Cloud Service Discovery	T1091 Replication Through Removable Media	T1602 Data from Configuration Repository	T1573 Encrypted Channel	T1011 Exfiltration Over Other Network Medium	T1561 Disk Wipe
T1597 Search Closed Sources	T1608 Stage Capabilities	T1053 Scheduled Task/Job	T1136 Create Account	T1484 Domain Policy Modification	T1484 Domain Policy Modification	T1006 Direct Volume Access	T1557 Man-in-the-Middle	T1613 Container and Resource Discovery	T1072 Software Deployment Tools	T1213 Data from Information Repositories	T1008 Fallback Channels	T1052 Exfiltration Over Physical Medium	T1495 Firmware Corruption
T1596 Search Open Technical Databases	T1195 Supply Chain Compromise	T1129 Shared Modules	T1543 Create or Modify System Process	T1611 Escape to Host	T1480 Execution Guardrails	T1556 Modify Authentication Process	T1482 Domain Trust Discovery	T1083 File and Directory Discovery	T1080 Data from Local System	T1005 Data from Local System	T1104 Multi-Stage Channels	T1567 Exfiltration Over Web Service	T1499 Inhibit System Recovery
T1593 Search Open Websites/Domains	T1199 Trusted Relationship	T1072 Software Deployment Tools	T1546 Event Triggered Execution	T1546 Event Triggered Execution	T1211 Exploitation for Defense Evasion	T1040 Network Sniffing	T1046 Network Service Scanning	T1550 Use Alternate	T1039 Data from	Non-Application Layer Protocol	T1029 Scheduled Transfer	T1498 Network Denial of Service	
T1504	T1078	T1569	T1133		T1222	T1003							



Interfaz gráfica



SIEVA

MITRE | ATT&CK SIEVA

MITRE | ATT&CK
DATA ANALYSIS
Mitre | Att&ck Matrix - Navigator

MITRE ATT&CK® × +

MITRE ATT&CK® × +

	TA0043 Reconnaissance 10 techniques	TA0042 Resource Development 7 techniques	TA0001 Initial Access 9 techniques	TA0002 Execution 12 techniques	TA0003 Persistence 19 techniques	TA0004 Privilege Escalation 13 techniques	TA0005 Defense Evasion 39 techniques	TA0006 Credential Access 15 techniques	TA0007 Discovery 27 techniques	TA0008 Lateral Movement 9 techniques	TA0009 Collection 17 techniques	TA0011 Command and Control 16 techniques	TA0010 Exfiltration 9 techniques	TA0040 Impact 13 techniques
T1595 Active Scanning	T1583 Acquire Infrastructure	T1189 Drive-by Compromise	T1059 Command and Scripting Interpreter	T1098 Account Manipulation	T1548 Abuse Elevation Control Mechanism	T1110 Brute Force	T1087 Account Discovery	T1210 Exploitation of Remote Services	T1560 Archive Collected Data	T1071 Application Layer Protocol	T1020 Automated Exfiltration	T1531 Account Access Removal		
T1592 Gather Victim Host Information	T1586 Compromise Accounts	T1190 Exploit Public-Facing Application	T1609 Container Administration Command	T1197 BITS Jobs	T1134 Access Token Manipulation	T1555 Credentials from Password Stores	T1010 Application Window Discovery	T1534 Internal Spearphishing	T1123 Audio Capture	T1092 Communication Through Removable Media	T1030 Data Transfer Size Limits	T1485 Data Destruction		
T1599 Gather Victim Identity Information	T1584 Compromise Infrastructure	T1184 Exploit Remote Services	T1160 Deploy Container	T1547 Boot or Logon Autostart Execution	T1547 Boot or Logon Autostart Execution	T1212 Exploitation for Credential Access	T1217 Browser Bookmark Discovery	T1570 Lateral Tool Transfer	T1119 Automated Collection	T1132 Data Encoding	T1048 Exfiltration Over Alternative Protocol	T1486 Data Encrypted for Impact		
T1590 Gather Victim Network Information	T1587 Develop Capabilities	T1200 Hardware Additions	T1203 Exploitation for Client Execution	T1037 Boot or Logon Initialization Scripts	T1037 Boot or Logon Initialization Scripts	T1187 Forced Authentication	T1580 Cloud Infrastructure Discovery	T1563 Remote Service Session Hijacking	T1115 Clipboard Data	T1001 Data Obfuscation	T1041 Exfiltration Over C2 Channel	T1565 Data Manipulation		
T1591 Gather Victim Org Information	T1585 Establish Accounts	T1566 Phishing	T1559 Inter-Process Communication	T1176 Browser Extensions	T1037 Boot or Logon Initialization Scripts	T1606 Forge Web Credentials	T1538 Cloud Service Dashboard	T1021 Remote Services	T1530 Data from Cloud Storage Object	T1568 Dynamic Resolution	T1491 Defacement	T1561 Disk Wipe		
T1598 Phishing for Information	T1590 Gather Victim Network Information	T1598 Obtain Capabilities	T1091 Replication Through Removable Media	T1543 Create or Modify System Process	T1543 Create or Modify System Process	T1056 Input Capture	T1526 Cloud Service Discovery	T1091 Replication Through Removable Media	T1602 Data from Configuration Repository	T1573 Encrypted Channel	T1011 Exfiltration Over Other Network Medium	T1499 Endpoint Denial of Service		
T1597 Search Closed Sources	T1591 Gather Victim Org Information	T1608 Stage Capabilities	T1106 Native API	T1136 Create Account	T1136 Create Account	T1557 Man-in-the-Middle	T1613 Container and Resource Discovery	T1072 Software Deployment Tools	T1213 Data from Information Repositories	T1008 Fallback Channels	T1052 Exfiltration Over Physical Medium	T1495 Firmware Corruption		
T1596 Search Open Technical Databases	T1598 Phishing for Information	T1195 Supply Chain Compromise	T1053 Scheduled Task/Job	T1543 Create or Modify System Process	T1543 Create or Modify System Process	T1484 Domain Policy Modification	T1482 Domain Trust Discovery	T1083 File and Directory Discovery	T1219 Data from Information Repositories	T1105 Ingress Tool Transfer	T1567 Exfiltration Over Web Service	T1498 Network Denial of Service		
T1593 Search Open Websites/Domains	T1597 Search Closed Sources	T1199 Trusted Relationship	T1129 Shared Modules	T1546 Event Triggered Execution	T1546 Event Triggered Execution	T1480 Execution Guardrails	T1083 File and Directory Discovery	T1040 Network Sniffing	T1083 File and Directory Discovery	T1104 Multi-Stage Channels	T1029 Scheduled Transfer			
T1594	T1594	T1078	T1569	T1133	T1133	T1222	T1003	T1046 Network Service Scanning	T1550 Use Alternate	T1039 Data from				



Interfaz gráfica



SIEVA

MITRE | ATT&CK

MITRE ATT&CK

TA0043 Reconnaissance	TA0 Reso Develo
10 techniques	7 techn
T1595 Active Scanning	T1583 Acquire Infrastruct
T1592 Gather Victim Host Information	T1586 Compromi Accounts
T1589 Gather Victim Identity Information	T1584 Compromi Infrastruct
T1590 Gather Victim Network Information	T1587 Develop C
T1591 Gather Victim Org Information	T1585 Establish
T1598 Phishing for Information	T1588 Obtain Cap
T1597 Search Closed Sources	T1608 Stage Cap
T1596 Search Open Technical Databases	
T1593 Search Open Websites/Domains	
T1594	

SIEVA

MITRE | ATT&CK DATA ANALYSIS Mitre | Att&ck Matrix - Data Visualization

dataset

index1

index2

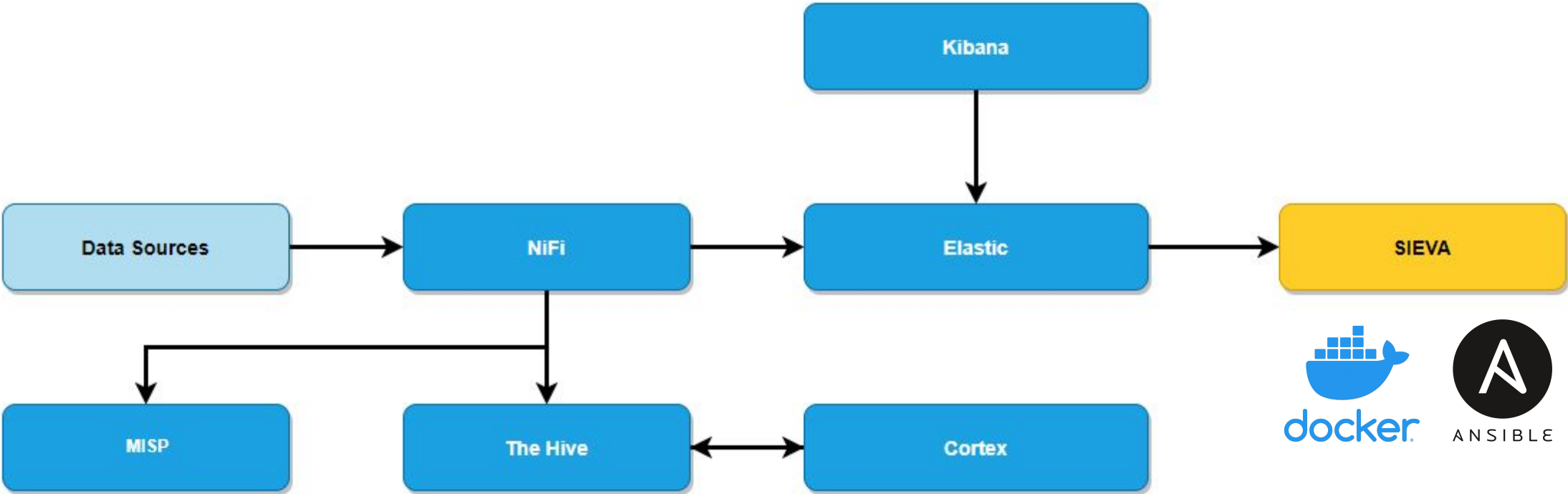
index3

Classification_validate_dataset

- FIREWALL**
FILENAME, PACKETS-SENT, URL, SOURCE, APPLICATION, PACKETS-RECEIVED, BYTES-SENT, BYTES-RECEIVED
- DNS**
IP, PROTOCOL, CODE, BYTES-SENT, URL, USER_AGENT
- WEBSERVER**
IP, URL, HTTP-CODE, HTTP-METHOD
- EVTX**
No Data
- IDENTITY**
No Data
- DHCP**
No Data



Integración en un SOC



Resumiendo



Cómo puede SIEVA ayudarte?

Reducir esfuerzos en ing. datos

Identificar lagunas en tu visibilidad

Mejorar estrategia de gestión de datos
y monitorización de amenazas



Disponible Open Source
Licencia AGPLv3



@i2CAT's Github SIEVA Repositorio
<https://github.com/Fundacio-i2CAT/SIEVA>



Q&A



nil.ortiz@i2cat.net

LinkedIn/in/nilortiz

Disponible Open Source
Licencia AGPLv3



@i2CAT's Github SIEVA Repositorio
<https://github.com/Fundacio-i2CAT/SIEVA>